App. No. 09/663,811
Amendment Dated June 27, 2006
Reply to Office Action of April 28, 2006

REMARKS

The claims have been amended as set forth above. Applicants assert that the claims are allowable over the Examiner's cited references. No new matter has been added.

I.   Examiner Interview Dated May 16, 2006

Applicants' attorney held an interview with Examiner Chen on May 16, 2006. During that interview, clarification of the term "domain" was discussed. Also, association of the "owner network domain" and the "object" was discussed. Applicants have amended the claims in light of the interview and believe the claims are now allowable over the cited references. Applicants request a second interview with Examiner Chen if, after reading this amendment, Examiner Chen believes that the claims are still unallowable.

II.   Rejection of Claims 1-3, 5-7, and 9-22 Under 35 U.S.C. 103(a)

All of the pending claims stand rejected under 35 U.S.C. 103(a) for being obvious based on U.S. Patent No. 5,469,556 issued to Clifton (hereinafter "Clifton") in combination with two or more other references. Applicants respectfully disagree with the rejection. Independent claim 1 has been amended to recite the following combination of elements no taught or otherwise suggested by the cited references:

> "...receiving, at a first computing machine, a request to modify an object associated with a shared data structure, wherein the shared data structure *is shared by the plurality of network domains*, wherein the first computing machine *resides in at least one of the network domains, wherein the object includes a security descriptor identifying an owner network domain of the object* and an identification of one or more users;
>
> determining whether the first computing machine *resides in the owner network domain* by retrieving from the security descriptor *the identity of the owner network domain and comparing the owner network domain identity to the network domain within which the first computing machine resides*; and
>
> *rejecting the request to modify the object when the first computing machine does not reside in the owner network domain.*"

Page 8 of 11

Independent claim 1 has been amended to recite a network domain associated with a

distributed computer network. Claim 1 has also been amended to recite that the object includes a

security descriptor identifying an owner network domain of the object. As one example of the

problems associated with the prior art and how aspects of the present invention overcome the

problems of the prior art, the disclosure of the present invention recites as follows:

> "An administrator in one domain with the appropriate privileges could, in the
> absence of the security safeguards made possible by the present invention,
> exercise certain privileges often granted to administrators. For example, an
> administrator (or other user) with a Take Ownership privilege could potentially
> take ownership of an object (including Schema data or Configuration data) in the
> directory service even though that administrator may not have access permission
> to the object. Once the administrator has taken ownership of the object, as
> mentioned above, the administrator can add any permissions desired to exercise
> complete control over the object. Moreover, the modification (because it is to an
> object within the directory service) would be replicated to each domain controller
> in the domain forest. In that way, a malicious administrator could cause much
> damage to otherwise secure configuration or schema data owned by
> administrators in other domains.
>
> Another security risk relates to the misuse of the Create Token and TCB
> privileges. Typically, those privileges are used by an administrator to
> impersonate another user or trusted process, such as for the purpose of
> temporarily granting permissions to an executing process. However, a malicious
> user with those privileges could create a token that identifies the malicious user as
> a member of a group that has access permission to a shared resource or object in
> the shared directory service (e.g., an administrator from another domain) and then
> attach that token to the malicious user's process. In that way, the malicious user
> could grant himself unauthorized access to shared objects. It is in view of these
> and other threats that the present invention, among other things, enables new
> security safeguards. The safeguards help prevent an administrator in one domain
> from performing unauthorized modifications on objects owned by a user in
> another domain, while maintaining the benefits of a distributed directory service,
> namely allowing enterprise-wide access and administration of shared resources."
> *Specification* at Page 12, line 20 through page 13, line 20.

The office action cites to Clifton as teaching the elements of independent claim 1.

Applicants respectfully assert that Clifton does not teach or suggest an owner network domain.

The cited portion of Clifton recites as follows:

> "The resource access security system of the present invention performs the
> translation of a descriptor by use of a user/job information table, including a

BEST AVAILABLE COPY

plurality of user/job entries, each having stored therein a user/job pointer which points to a base address of a domain table to which the user/job has the privilege of access, a plurality of domain tables, each including a plurality of domain entries, wherein each domain entry has stored therein a domain pointer which points to a base address of a page table and a plurality of page tables, each having a plurality of pages wherein each page has stored therein a base address of a resource in the address space of the data processing computer to which access is sought.

The user/job table referenced above is used to obtain user/job information related to the requested resource and related to the user or job seeking access to the resource. The user/job information points to *a domain table containing the privilege levels or domains to which the user or job has the privilege of access. The domain tables are used to obtain the particular domain or privilege level of the user or job.* The page tables are used to obtain the page of resources included in the identified domain." *Clifton,* at column 3, line 54 to column 4, line 8 (emphasis added).

As can be seen from the emphasized portion of the cited Clifton text, the domain table contains privilege levels or domains of a user or job. The domain of a user or job is not equivalent to an owner network domain, as recited in the claims.

The office action also cites to U.S. Patent No. 6,839,843 issued to Bacha et al. (hereinafter "Bacha"). The office action asserts that even if Clifton does not teach the element "owner domain" Bacha teaches this element. Applicants respectfully traverse this assertion. The cited portion of Bacha teaches as follows:

"In another aspect, the present invention provides a system and method for securely authenticating user access to electronic data stored in a data repository managed by a repository manager unrelated to a source of the data, in which an access control list of user authorizations is associated with the electronic data when stored in the data repository. The source is responsible for updating the access control list, and maintains evidence of the current access control list. Evidence of the current access control list is also provided to any user computer which has effected the update. The source verifies that the updated access control list stored with the electronic data in the data repository is accurate before releasing the data to the requesting computer." *Bacha,* at Column 3, lines 3-25.

Applicants can find no teaching or suggestion in Bacha of the elements recited above in independent claim 1. Accordingly, Applicants believe that independent claim 1 is allowable over the Examiner's cited references.

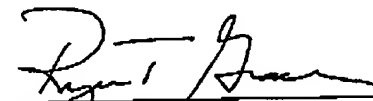Page 10 of 11

BEST AVAILABLE COPY

With regard to independent claims 7 and 13, Applicants rely on the assertions set forth above in support for independent claim 1. Regarding dependent claims 2, 3, 5-6, 9-12, and 14-22, applicants believe that those claims include elements not taught or otherwise suggest by the cited reference. Also, those claims ultimately depend from independent claims 1, 7, and 13, respectively. In light of their dependency, Applicants believe that those claims are allowable for at least the same reasons set forth above.

III.   Request for Reconsideration

In view of the foregoing amendments and remarks, all pending claims are believed to be allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the applicant at the telephone number provided below.

Respectfully submitted,

MERCHANT & GOULD P.C.

Ryan T. Grace
Registration No. 52,956
Direct Dial: 206.342.6258

MERCHANT & GOULD P.C.
P. O. Box 2903
Minneapolis, Minnesota 55402-0903
206.342.6200

27488
PATENT TRADEMARK OFFICE

Page 11 of 11

PAGE 14/14 * RCVD AT 6/27/2006 5:52:04 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/22 * DNIS:2738300 * CSID:206 342 6201 * DURATION (mm-ss):03-32